FI0001059648

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 105964 B

(45) Patentti myönnetty - Patent beviljats 31.10.2000

(51) Kv.lk.7 - Int.kl.7
H04L 9/14

(21) Patenttihakemus - Patentansökning 990757

(22) Hakemispäivä - Ansökningsdag 06.04.1999

(24) Alkupäiva - Löpdag 06.04.1999

(41) Tullut julkiseksi - Blivit offentlig 17.06.2000

(32) (33) (31) Etuoikeus - Prioritet

16.12.1998 FI 982727 P

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •**Nokia Networks Oy,** Helsinki, Keilalahdentie 4, 02150 Espoo, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •**Einola, Heikki,** Kaksoiskiventie 7-9 B 5, 02760 Espoo, SUOMI - FINLAND, (FI)
2 •**Rajaniemi, Jaakko,** Lapinrinne 2 A 11, 00180 Helsinki, SUOMI - FINLAND, (FI)
3 •**Hulkkonen, Tony,** Kauppakartanonkatu 26 H 93, 00930 Helsinki, SUOMI - FINLAND, (FI)
4 •**Bäck, Juha,** Kulosaaren Puistotie 44 B 22, 00570 Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Nokia IPR-osasto
PL 319
00045 Nokia Group

(54) Keksinnön nimitys - Uppfinningens benämning

Menetelmä matkaviestinyhteyksien hallintaan
Förfarande för hantering av mobilteleförbindelser

(56) Viitejulkaisut - Anförda publikationer

EP A 0869692 (H04Q 7/38, ICO Services Ltd., palsta 1 rivi 1 - palsta 5 rivi 54, palsta 11 rivi 24 - palsta 13 rivi 56, kuvat 8 ja 11, palsta 14 rivit 1 - 52), US A 5729537 (H04L 9/32, Telefonaktiebolaget L M Ericsson (publ), palsta 5 rivi 59 - palsta 11 rivi 62), US A 5878036 (H04B 7/216, Michael K. Spartz, Daniel H. Agre, Barry R. Robbins, palsta 3 rivi 48 - palsta 5 rivi 35, palsta 15 rivi 25 - palsta 16 rivi 6, palsta 19 rivit 19 - 45, palsta 24 rivit 24 - 67, palsta 26 rivit 5 - 31, palsta 26 rivit32 -59), WO A 9933299 (H04Q 7/38, Siemens Aktiengesellschaft, sivu 10 rivit 1 - 25, sivu 3 rivi 17 - sivu 4 rivi 4, sivu 11 rivi 4 - sivu 12 rivi 2)

(57) Tiivistelmä - Sammandrag

Esillä oleva keksintö on uusi ja parannettu menetelmä tietyn matkaviestimen ja useiden runkoverkkojen tai runkoverkko-kokonaisuuksien välisen liikennöinnin salaamiseen käytettävien salausavaimien ja -algoritmien hallitsemiseen yhdestä paikasta. Vielä eräässä toisessa keksinnön toteutustavassa hallinnan sijaintipaikka on liikkuva matkaviestimen liikkuessa radioliittymäverkon alueella.

Föreliggande uppfinning är ett nytt och förbättrat förfarande för hantering på ett och samma ställe av chiffernycklar och algoritmer för kryptering eller chiffrering av kommunikationen mellan en mobilstation och flera kärnnät och kärnnätsenheter. Dessutom är hanteringsplatsen flyttbar i och med att mobilstationen flyttar sig inom radioaccessnätet.

Menetelmä matkaviestinyhteyksien hallintaan

KEKSINNÖN TEKNINEN SOVELTAMISALUE

Esillä oleva keksintö liittyy salaamiseen ja salauksen purkuun kykeneviin viestintäverkkoihin ja erityisesti avainten hallintamenetelmään tällaisissa tietoliikenneverkoissa.

KEKSINNÖN TAUSTA

Radioteitse tapahtuva siirto on luonnostaan alttiimpaa salakuuntelulle ja väärennöksille kuin kiinteä langallinen tietoliikenne. Liikenteen kuunteleminen on helppoa eikä vaadi pääsyä erityisiin tiloihin. GSM solukkojärjestelmässä tätä ongelmaa on vähennetty ottamalla käyttöön tunnistus ja salaaminen. Seuraavassa selitetään lyhyesti GSM:n tunnistamis- ja salausmenettelyt viitaten Kuvioon 1. Yksityiskohtaisempi kuvaus löytyy esimerkiksi julkaisusta "The GSM system for mobile communications", Mouly et. al.

Kuvio 1 havainnollistaa nykyistä GSM-järjestelmää, johon sisältyy yleinen pakettiradiopalvelu- eli GPRS -verkko. Täydellinen verkko käsittää kolme eri toiminnallista aliverkkoa, radioliittymäverkon, piirikytkentäisen eli ensimmäisen runkoverkon ja pakettikytkentäisen eli toisen runkoverkon. Radioliittymäverkko käsittää tukiasemaohjaimia eli BSC:iä 30 (kuviossa vain yksi) ja tukiasemia eli BS:iä 20. Ensimmäisen runkoverkko käsittää matkapuhelinkeskuksia vierailijarekistereineen eli MSC/VLR:iä 40 ja kotirekisterejä tunnistuskeskuksineen eli HLR/AuC:iä 50. Ensimmäisen runkoverkko käsittää lisää MSC/VLR:iä ja HLR/AuC:iä, joita ei selkeyden takia ole esitetty kuviossa. Toinen runkoverkko käsittää yleisen pakettiradiopalveluverkon palvelusolmun eli SGSN:n Toinen runkoverkko käsittää lisää yleisen pakettiradiopalveluverkon palvelusolmuja eli GSN:iä, joita ei selkeyden takia ole esitetty kuviossa. Molemmat runkoverkot voivat käyttää yhteistä kotirekisteriä tunnistuskeskuksineen eli HLR/AuC:tä.

Kun käyttäjälaite UE (eli matkaviestin MS) 10 liittyy ensimmäiseen runkoverkkoon se rekisteröi itsensä MSC/VLR:än 40. Saatuaan rekisteröinti- tai palvelupyynnön matkaviestimeltä, MSC/VLR 40 lähettää HLR/AuC:lle pyynnön, joka sisältää IMSI:n, saadakseen tunnistustripletin, jotka muodostavat RAND, SRES ja Kc1. GSM:ssä MM eli liikkuvuuden hallintaprotokolla suorittaa tunnistuksen toiminnallisuuden. Tripletit ovat ennalta määrätyn pituisia ja ne lasketaan käyttäen salaista avainta Ki, jonka tuntevat ainoastaan tunnistuskeskus ja matkaviestimessä oleva SIM-kortti. Vastaanotettuaan tripletit HLR/AuC:ltä MSC/VLR lähettää kutsun, RAND, MS:lle tunnistuspyynnössä tuon kyseisen MS:n tunnistamiseksi. Osana onnistunutta rekisteröintiä MSC/VLR päivittää MS:n sijainnin HLR:in ja lukee tilaajatiedot HLR:stä.

Matkaviestimellä 10 on salainen avain Ki SIM-kortissaan. Palvelun tarjoaja tallentaa verkkoon liityttäessä salaisen avaimen Ki, eikä tilaaja tai kukaan muukaan näe sitä. Se on identtinen tunnistuskeskukseen 50 tallennetun salaisen avaimen Ki kanssa. Salaista avainta Ki sovelletaan yhdessä satunnaisluvun RAND kanssa ennalta määrättyyn algoritmiin nimeltään A3 allekirjoitetun vasteen SRES muodostamiseksi. Matkaviestin 10 lähettää sen jälkeen SRES:in sisältävän sanoman MSC/VLR:lle 40, joka vertaa sitä AuC:lta 50 vastaanotettuun SRES:in. Jos vertailu on onnistunut, matkaviestin 10 on tunnistettu ja sen pääsy verkkoon sallitaan. Samanaikaisesti kun SRES lasketaan matkaviestin syöttää RAND:in ja Ki:n toiseen ennalta määrättyyn algoritmiin nimeltään A8 salausavaimen Kc1 muodostamiseksi. Jos tunnistus onnistui ja verkko niin päättää, kaikki tämän jälkeen matkaviestimen 10 kanssa ilmarajapinnan kautta tapahtuva tietoliikenne salataan.

Tätä varten MSC/VLR lähettää salausavaimen Kc1 matkaviestimen 10 kanssa liikennöivälle BSC:lle ja BSC vuorostaan toimittaa Kc1:n edelleen MS:n kanssa liikennöivälle BTS:lle ja salaaminen tapahtuu tukiasemassa ja matkaviestimessä vielä erään algoritmin, esim. A5, mukaisesti. Kun MSC/VLR on päättänyt että

salausta käytetään, BSC tekee päätöksen käytettävästä algoritmista. GSM:ssä on tällä hetkellä valittavissa kaksi salausalgoritmia.

Jos matkaviestin 10 haluaa päästä toiseen runkoverkkoon, se rekisteröi itsensä SGSN:ssä 60. Tunnistusmenettely on samanlainen kuin menettely ensimmäisen runkoverkon yhteydessä, paitsi että salausavainta Kc2 ei lähetetä sille tukiasemalle (järjestelmän BSS-osalle), joka parhaillaan liikennöi matkaviestimen 10 kanssa. Toisin sanoen, salaaminen tapahtuu SGSN:ssä ja MS:ssä. SGSN 60 pitää salausavaimen Kc2 itsellään ja suorittaa salaamisen.

Tämän takia tekniikan tason mukainen järjestelmä käyttää eri salausavaimia kahden eri runkoverkon välisen liikennöinnin salaamiseen ja salaamista sovelletaan kahteen erilliseen radioyhteyteen sillä MSC:n ja SGSN:n kanssa liikennöintiin käytetään eri radiokanavia. Tämän tuloksena GSM MS, joka liikennöi samanaikaisesti sekä MSC:n että SGSN:n kanssa hyödyntää kahta salausavainta kahdella eri radiokanavalla tai yhteydellä, joilla molemmilla on verkossa oma itsenäinen valvontansa.

Se tosiasia että salaaminen ja salaamisen ohjaus tapahtuvat eri paikoissa voi aiheuttaa yhteensopivuusongelmia. Se, että radioliittymäverkko ei pääse lainkaan käsiksi toisen runkoverkon signalointisanomiin voi osoittautua ongelmalliseksi tulevissa verkoissa, kun kaikkia tietyn käyttäjän käyttämiä radioresursseja tulisi hallita yhteistoiminnassa järjestelmässä jossa on kaksi salaamista ohjaavaa CN -solmua. Tässä tapauksessa samanaikaisiin yhteyksiin MSC:hen ja SGSN:än varattuja radioresursseja hallitsisi yksi kokonaisuus järjestelmän radioliittymäverkko-osassa, mutta kuitenkin salaamista ohjaamassa olisi kaksi kokonaisuutta.

On ehdotettu että UMTS:ssä tulisi olemaan vain yksi RRC eli radioresurssin ohjausprotokolla, joka ohjaa sekä yhteyttä MSC:hen että SGSN:än. Jos käytetään vain yhtä avainta kerrallaan molempiin yhteyksin, ongelmana on, miten

viestittää toiselle CN -solmulle, että sen avainta ei tulla käyttämään. Vielä toinenkin ongelma liittyy CN -kokonaisuuden ohjaamiin kanavanvaihtoihin.

Siksi esillä olevan keksinnön tavoitteena on hallita tehokkaasti eri runkoverkkojen ja matkaviestimen välillä siirretyn käyttäjädatan salaamiseen ja salauksen purkamiseen käytettäviä salausavaimia ja -algoritmeja.

Esillä olevan keksinnön eräänä toisena tavoitteena on lisäksi hallita tehokkaasti eri runkoverkkojen ja matkaviestimen välillä siirretyn signalointidatan salaamiseen ja salauksen purkamiseen käytettäviä salausavaimia ja -algoritmeja.

Vielä eräänä esillä olevan keksinnön tavoitteena on siirtää tehokkaasti salausparametrit kun palveleva radioverkon ohjain luovutetaan toiselle radioverkon ohjaimelle, josta tällöin tulee uusi palveleva radioverkon ohjain.

YHTEENVETO KEKSINNÖSTÄ

Esillä oleva keksintö on uudenlainen ja parannettu menetelmä tietyn matkaviestimen ja useiden runkoverkkojen tai runkoverkkokokonaisuuksien välisen liikennöinnin salaamiseen käytettävien salausavaimien ja -algoritmien hallitsemiseksi tehokkaasti yhdestä paikasta. Vielä eräs keksinnön toteutustapa on se, että hallinnan sijaintipaikka voi siirtyä matkaviestimen liikkuessa radioliittymäverkon alueella.

Esillä olevan keksinnön edullinen toteutusmuoto liittyy 3:nnen sukupolven matkaviestinverkkoon, josta käytetään lyhenteitä UMTS tai WCDMA. Verkko on esitetty Kuviossa 2. Verkko käsittää useita aliverkkoja. Radioliittymäverkko eli UTRAN (UMTS Terrestrial Radio Access Network) käsittää useita radioverkko-ohjaimia eli RNC:itä 130, joista kukin ohjaa useita tukiasemia eli BS:iä 120. Ensimmäinen runkoverkko käsittää matkapuhelinkeskuksen vierailijarekistereineen eli MSC/VRL:n 140 ja kotirekisterin tunnistuskeskuksineen

eli HLR/AuC:n 150. Ensimmäinen runkoverkko käsittää muitakin MSC/VRL:iä ja HLR/AuC:ia, joita ei selkeyden takia ole esitetty. Toinen runkoverkko on pakettiverkko ja se käsittää palvelevan GPRS tukisolmun eli SGSN:n 160. Toinen runkoverkko käsittää lisäksi GPRS reittitukisolmuja eli GGSN:iä, joita ei selkeyden takia ole esitetty. Huomattakoon että UTRAN voi olla liitetty toisen palvelun tarjoajan runkoverkkoon tai kolmanteen runkoverkkoon joka on samanlainen kuin ensimmäinen runkoverkko.

Koska ilmarajapinnan yhteysmenetelmä on CDMA, matkaviestin 110 kykenee liikennöimään samanaikaisesti useiden tukiasemien kanssa (tätä kutsutaan pehmeäksi tai monitiekanavanvaihdoksi. Kun tämä tapahtuu, kaikki lähetykset matkaviestimestä 110 ohjataan yhteen RNC:hen, jota kutsutaan palvelevaksi RNC:ksi eli SRNC:ksi, jossa lähetykset yhdistetään yhdeksi lähetykseksi lähetettäväksi edelleen haluttuun runkoverkkoon. Lisäksi SRNC hallitsee radioyhteyksiä.

Edullisessa toteutusmuodossa matkaviestin muodostaa liikenneyhteyden yhden runkoverkon tai runkoverkkokokonaisuuden kanssa tai päinvastoin. Yhteyttä perustettaessa verkko pyytää matkaviestintä tunnistamaan itsensä, kuten edellä on selitetty. Samanaikaisesti tunnistamisen kanssa matkaviestin ja verkko (eli CN -solmu) laskevat identtiset salausavaimet Kc1. Keksinnön edullisessa toteutusmuodossa se runkoverkko tai runkoverkkokokonaisuus, joka laski salausavaimen ei aloita käyttäjädatan tai signalointisanomien salaamista vaan muodostaa ja lähettää sanoman joka käsittää avaimen ja käytettävän algoritmin ilmaisevan datan salausohjaimelle 180, joka edullisesti sijaitsee palvelevassa radioverkko-ohjaimessa. Salausohjain vastaanottaa mainitun sanoman ja alkaa salata runkoverkosta matkaviestimeen päin virtaavia data- ja signalointisanomia, sekä purkaa matkaviestimestä runkoverkkoon päin virtaavien data- ja signalointisanomien salausta.

Keksinnön edullisessa toteutusmuodossa toinen runkoverkko tai runkoverkko-kokonaisuus voi aloittaa liikennöinnin matkaviestimen kanssa, tai päinvastoin,

samalla kun liikenne ensimmäisen runkoverkon kanssa on vielä käynnissä. Toinen runkoverkko tai runkoverkkokokokonaisuus tunnistaa matkaviestimen ja toiset salausavaimet Kc2 lasketaan. Sen jälkeen, kuten edellä on kuvattu, toinen runkoverkko tai runkoverkkokokokonaisuus muodostaa ja lähettää salausohjaimelle sanoman joka käsittää toisen avaimen ja toisen avaimen kanssa käytettävän algoritmin ilmaisevan datan. Salausohjain vastaanottaa mainitun toisen sanoman ja vertaa ensimmäistä ja toista salausavainta, sekä niihin liittyviä algoritmeja. Jos ensimmäinen ja toinen salausavain niihin liittyvine algoritmeineen ovat yhtä luotettavia, salausohjain salaa ensimmäisen ja toisen runkoverkon välisen datan ja signalointisanomat, sekä purkaa niiden salauksen käyttäen sitä avainta ja algoritmia jota se käytti jo ennestään. Tämä on havainnollistettu Kuviossa 3. Kuitenkin, jos toinen salausavain ja siihen liittyvä algoritmi tarjoavat parannetun salauksen tai samaa avainta ei haluta enää käyttää (vaikka laatu tai salauksen lujuus olisivat samat), salausohjain alkaa käyttää toista avainta ja siihen liittyvää algoritmia myös liikennöinnissä ensimmäisen runkoverkon kanssa. Tämä on havainnollistettu Kuviossa 4. Kuviossa 3 esitetty tilanne voi aiheuttaa että samaa avainta käytetään hyvin kauan, sillä toiminta voi ketjuuntua MSC:n ja SGSN:n välillä. Tarve tai halu vaihtaa avain johtaa siihen että salausohjain muodostaa ja lähettää MS:lle sanoman joka käskee MS:n toimimaan tämän mukaisesti.

Esillä olevan keksinnön eräässä toisessa toteutusmuodossa vastaavia eri avaimia käytetään käyttäjädatan salaamiseen eri yhteyksillä, mutta korkeamman salaamiskyvyn omaavaa avainta ja siihen liittyvää algoritmia käytetään salaamaan molempiin runkoverkkoihin lähetetyt ja niistä tulevat signalointisanomat.

Vielä eräässä toteutusmuodossa, vastaanotettuaan toisen salausavaimen Kc2 sisältävän sanoman, salauksen ohjaus kuittaa mainitun sanoman toisella sanomalla, joka sisältää valitun salausavaimen ja algoritmin ilmaisevan informaation. Käytettävän avaimen viestittäminen toiseen CN -solmuun voi myös tapahtua alkuperäisen sanoman vastaanotossa osana COMPLETE LAYER 3 INFO -sanomaa. Näin menetellen toinen CN saa välittömästi tietoonsa, että

signalointiin tarkoitettu radioyhteys on jo salattu ja sen takia ei ole tarpeen kehottaa aloittamaan salausta.

Eräässä muussa toteutusmuodossa on vain yksi CN:ssä tapahtuvaa salaamista ohjaava kokonaisuus. Tämä lähestymistapa on havainnollistettu Kuviossa 6. Tässä tapauksessa ei ole tarvetta edellä kuvattuun avainten hallintaan RNC:ssä. Tämän tuloksena tilanne on RNC:n kannalta sama kuin tekniikan tason mukaisessa GSM järjestelmässä. Kuitenkin, CN:n puolella tilanne on uusi, sillä yksi kokonaisuus hallinnoi sekä MSC:n että SGSN:n tarjoamia palveluja (ja protokollia). Tällaisessa järjestelyssä on järjestelmälle tunnusomaista että GSM:ssä MSC:lle ja SGSN:lle kiinteästi kuuluviin yhteyksiin ja palveluihin kuuluvaa salaamista hallitsee mainittu yksi CN-kokonaisuus, joka käyttää yhtä signalointivirtaa radioliittymäverkon ja runkoverkon välillä, eli Iu-rajapinnassa.

Eräässä muussa toteutusmuodossa CN:n kahden salauksen ohjauskokonaisuuden välillä on rajapinta, joka huolehtii tarvittavasta koordinoinnista. Käytännössä MSC:n ja SGSN:n välillä voisi olla rajapinta nimeltään Gs. Sellaisenaan Gs on olemassa tekniikan tason mukaisessa GSM järjestelmässä, mutta se ei sisällä salausavaimia koordinoivaa toiminnallisuutta. Kuvio 7 havainnollistaa erästä laajennetun Gs-rajapinnan tarjoaman koordinoinnin toteutusmuotoa tai -tapaa. Aktiviteettikyselyn vaste voi sisältää myös muuta dataa, kuten SRNC ID:n haun välttämiseksi MT-tapauksessa sellaisissa RNC:issä jotka eivät ole palvelevia, mutta kuuluvat siihen LA/RA:han johon päätelaite on sillä hetkellä rekisteröitynyt.

Esillä olevan keksinnön edullisessa toteutusmuodossa on mahdollista, että liikenne matkaviestimelle reititetään uudelleen toisen palvelevan radioverkko-ohjaimen kautta. Jos näin tapahtuu, pitää salaukseen ja salauksen purkuun käytettävät parametrit (muiden kohdeohjaimen kautta liikennöinnin aloittamisen tarvittavien parametrien lisäksi) siirtää CN:n kautta salausohjaimen uuteen sijaintipaikkaan. Tämä tehdään signaloimalla parametrit tai niitä koskeva informaatio läpinäkyvästi vastaavien runkoverkkojen kautta. Vaihtoehtoisesti

tämä voidaan tehdä signaloimalla parametrit radioverkko-ohjaimien välisen lu-rajapinnan kautta.

LYHYT KUVIOIDEN KUVAUS

Keksintö kuvataan seuraavassa yksityiskohtaisemmin viitaten oheisiin kuvioihin, joista

Kuvio 1 havainnollistaa tekniikan tason mukaista matkaviestinjärjestelmää,

Kuvio 2 esittää esillä olevan keksinnön edullisen toteutusmuodon mukaista UMTS-verkkoa,

Kuvio 3 havainnollistaa yhden salausavaimen valintaa kaikkea liikennöintiä varten,

Kuvio 4 havainnollistaa tapausta, jossa salausavain vaihdetaan liikennöinnin aikana,

Kuvio 5 havainnollistaa signalointijaksoa SRNC:n uudelleen sijoituksessa,

Kuvio 6 havainnollistaa tapausta, jossa on vain yksi runkoverkon salaamiskokonaisuus,

Kuvio 7 havainnollistaa aktiviteettikyselyä ensimmäisestä runkoverkkokokokonaisuudesta toiseen runkoverkkokokokonaisuuteen,

Kuvio 8 havainnollistaa vaihtoehtoista signalointijaksoa SRNC:n uudelleen sijoituksessa.

Samoja viitenumeroja käytetään kuvioiden samanlaisista kokonaisuuksista.

YKSITYISOHTAINEN KUVAUS

Salaaminen tapahtuu todennäköisesti UTRAN:in puitteissa UMTS:ssä. Kahdessa MM-vaihtoehdossa on kaksi kokonaisuutta, eli MSC ja SGSN, jotka voivat pyytää salausta radiorajapinnassa.

Oletetaan että UMTS:ssä CN pääosoitteet antavat UTRAN:ille salausavaimen ja sallitut salausalgoritmit tavallisesti yhteyden alussa. Salaamiskäskysanoman vastaanottaminen UTRAN:issa aiheuttaa radiorajapinnan salaamiskäskysanoman muodostamisen ja, mikäli mahdollista, kutsuu salaamislaitetta aloittamaan datavirran salaamisen. CN pääosoitteelle ilmoitetaan onko salaaminen suoritettu onnistuneesti radiorajapinnassa, sekä valittu salausalgoritmi.

Kun uusi yhteys perustetaan toisesta CN-pääosoitteesta, jolla ei ole mitään yhteyttä UE:hen, uusi CN-pääosoite toimittaa myös salausavaimen ja käytettäviksi sallitut salausalgoritmit UTRAN:ille yhteyden alussa. Tämä johtuu siitä, että CN-pääosoitteet ovat salausmielessä toisistaan riippumattomia.

Jos oletetaan, että kaikkiin yhteyksiin käytetään vain yhtä salausavainta ja yhtä salausalgoritmia, tämä johtaa tilanteeseen, jossa salausavaimia on enemmän (kaksi) kuin CN-pääosoitteista toimitettu yksi salausavain ja vain yhtä niistä käytetään.

Tämä tilanteen hoitamiseksi UTRAN:in pitää valita jompikumpi salausavaimista. Jos kahden CN-pääosoitteen pyytämien salausvaatimusten välillä ei ole eroja tai avainta ei haluta vaihtaa, silloin säilytetään esim. ensimmäinen salausavain ja algoritmi, kuten Kuviossa 3 esitetään.

Kahden CN-pääosoitteen välisen salausavaimen valitsemisen seurauksena (jos molemmilla CN-pääosoitteilla on aktiivinen yhteys/yhteydet UE:hen) jompikumpi

CN-pääosoitteista ei tiedä yhteyteen/yhteyksiin käytettävää oikeaa salausavainta. Vain UTRAN ja UE tietävät käytettävän oikean salausavaimen.

Voi olla tarpeen käyttää yhtä salausavainta esim. yhtä radioyhteyden kantajaa varten. Eri käyttäjätasojen kantajat salataan eri salausavaimilla, jotka toimittaa vastaavasti yksi CN-pääosoite. Tämä tarkoittaa, että esim. kahta MSC:n kautta kulkevaa puhelua varten datavirtoihin käytettäisiin kahta avainta. Kuitenkin, ohjaustasolla käytetään vain yhtä salausavainta ja siksi ohjaustasolla pitää olla koordinointi CN-pääosoitteiden tai -osoitteen toimittamien avaimien välillä.

Koordinointi ohjaustasolla on samanlainen kuin se, joka on esitetty UTRAN:issa käytetylle yhdelle salausavaimelle. Ohjaustasolla UTRAN:in pitää valita jompikumpi CN-pääosoitteiden toimittamista salausavaimista jos molemmat CN-pääosoitteet ovat aktiivisina, tai CN-pääosoitteen toimittamista jos useampi kuin yksi kantaja on käytössä.

GSM-järjestelmässä, kun BSC:ien välinen kanavanvaihto suoritetaan, MSC lähettää salausavaimen ja sallitut algoritmit kohde-BSC:hen BSSMAP HANDOVER REQUEST -sanomassa. GPRS:ssä, koska SGSN suorittaa salaamisen, BSC:ien välinen kanavanvaihto ei aiheuta mitään salausavaimen hallinnan tarvetta.

UMTS:ssä ei GSM-lähestymistapaa voida soveltaa palvelevien RNC:ien (SRNC) uudelleen sijoittamiseen, sillä CN-pääosoitteet eivät välttämättä tiedä käytettävää oikeaa salausavainta, kuten edellä on kuvattu. Ratkaisuna on välittää salaustieto CN:n kautta läpinäkyvästi kun SRNC uudelleensijoitetaan.

Kuvio 4 kuvaa salausavainsignalointia RNC:ien välisessä kanavanvaihdossa. Salausavain siirretään (CN:lle) läpinäkyvässä UTRAN-informaatiokentässä lähde-RNC:stä kohde-RNC:lle RANAP SRNC REQUIRED ja RANAP SRNC REQUEST sanomissa. Täten oikea salausavain siirretään kohde-RNC:lle.

Kanavanvaihdossa UMTS:ltä GSM:lle salausavainta ei voida siirtää läpinäkyvästi, kuten on ehdotettu UMTS:n suhteen. CN:n (tai IWU:n) on muodostettava BSSMAP HO REQUEST sanoma, jossa on MSC:ltä saatu salausavain. 2G-SGSN vastaanottaa salausavaimensa vanhalta 3G-SGSN:ltä Gn-rajapinnan kautta, kuten tapahtuu GPRS:ssä.

Jos UMTS:ssä käytetyt salausavaimet ovat erilaisia kuin GSM:n, esim. salausavaimen pituus on erilainen, sekä MSC:n että SGSN:n salausavaimet pitää vaihtaa UMTS-GSM kanavanvaihdossa.

GSM:ssä A-rajapinta BSSMAP tukee läpinäkyvää kenttää BSSMAP HO REQUIRED ja BSSMAP HO REQUEST sanomissa, mikä sallii ehdotetun ratkaisun hyödyntämisen myös UTRAN:in liitetyssä GSM CN:ssä.

Eräs vaihtoehtoinen signalointi on esitetty Kuviossa 8. Tässä tapauksessa avaimia hallinnoidaan kuten MSC:ssä GSM-järjestelmässä (kuvattu edellä), mutta läpinäkyvä informaatio sisältää ilmaisun siitä mikä avain on käytössä. Esimerkiksi, jos SGSN:n toimittama avain oli käytössä lähteessä, kohde vastaanottaisi kaksi avainta sekä tiedon siitä, että SGSN:n avain on käytössä. Tämän vaihtoehdon etuna on sen samankaltaisuus GSM:n kanssa, mikä helpottaa kanavanvaihtoa GSM:n kanssa, sillä avaimenhallintaperiaate CN:ssä (itse asiassa vain MSC:ssä) on sama sekä GSM:ssä että UMTS:ssä.

Edellä esitetyn kuvauksen valossa alan ammattimiehelle on selvää, että edellä kuvattuun toteutusmuotoon voidaan tehdä muutoksia poikkeamatta esillä olevan keksinnön tunnusmerkeistä. Vaikka esillä olevan keksinnön edullinen toteutusmuoto on kuvattu yksityiskohtaisesti, on ilmeistä, että keksintöön on mahdollista tehdä lukuisia erilaisia muutoksia ja muunnoksia jotka kaikki kuuluvat keksinnön piiriin.

Patenttivaatimukset

1. Tietoliikenneverkko käsittäen käyttäjälaitteen, yhteysverkon ja useita runkoverkkoja, jossa mainittu käyttäjälaite pystyy liikennöimään samanaikaisesti ainakin kahden runkoverkon kanssa mainituista useista runkoverkoista, **tunnettu** siitä, että ainakin kaksi mainituista useista runkoverkoista käsittää kukin välineet erillisten salausparametrien viestittämiseksi mainittuun yhteysverkkoon; ja mainittu yhteysverkko käsittää välineet yhden mainituista erillisistä salausparametreistä valitsemiseksi liikenteen salaamiseksi mainitun käyttäjälaitteen ja mainittujen ainakin kahden useista runkoverkoista välillä.

2. Patenttivaatimuksen 1 mukainen tietoliikenneverkko, **tunnettu** siitä, että mainittu yhteysverkko edelleen käsittää välineet mainitun liikenteen salaamiseen mainitun käyttäjälaitteen ja mainittujen ainakin kahden useista runkoverkoista välillä käyttäen mainittua yhtä mainituista erillisistä salausparametreistä.

3. Patenttivaatimuksen 1 tai 2 mukainen tietoliikenneverkko, **tunnettu** siitä, että mainittu salausparametri on salausavain tai salausalgoritmi tai molempien yhdistelmä.

4. Salaamismenetelmä tietoliikenneverkossa, joka käsittää käyttäjälaitteen, yhteysverkon ja useita runkoverkkoja, jossa mainittu käyttäjälaite pystyy liikennöimään samanaikaisesti ainakin kahden runkoverkon kanssa mainituista useista runkoverkoista, **tunnettu** siitä, että ainakin kaksi mainituista useista runkoverkoista käsittää kukin välineet erillisten salausparametrien viestittämiseksi mainittuun yhteysverkkoon; ja että mainittu yhteysverkko valitsee yhden mainituista erillisistä salausparametreistä liikenteen salaamiseen mainitun käyttäjälaitteen ja mainittujen ainakin kahden useista runkoverkoista välillä.

5. Patenttivaatimuksen 4 mukainen salaamismenetelmä, **tunnettu** siitä, että mainittu yhteysverkko lisäksi salaa liikenteen mainitun käyttäjälaitteen ja mainittujen ainakin kahden useista runkoverkoista välillä käyttäen valittua yhtä mainituista salausparametreistä.

6. Patenttivaatimuksen 4 tai 5 mukainen salaamismenetelmä, **tunnettu** siitä, että mainittu salausparametri on salausavain tai salausalgoritmi tai molempien yhdistelmä.

7. Patenttivaatimuksen 4 mukainen salaamismenetelmä, **tunnettu** siitä, että mainittu yhteysverkko käsittää useita kokonaisuuksia, jotka on tarkoitettu hallitsemaan yhteyksien salaamista vastaaville kokonaisuuksille sijoitetuilla maantieteellisillä alueilla sijaitseviin käyttäjälaitteisiin, ja että kun mainittu käyttäjälaite siirtyy eräälle ensimmäiselle salauksen hallintakokonaisuudelle sijoitetulta maantieteelliseltä alueelta toiselle salauksen hallintakokonaisuudelle sijoitetulle maantieteelliselle alueelle, mainittu ensimmäinen salauksen hallintakokonaisuus viestii käytetyt salausparametrit mainitulle toiselle salauksen hallintakokonaisuudelle signaloimalla käyttäen ainakin kahta mainituista useista runkoverkoista.

8. Yhteysverkko, joka on liitetty useisiin runkoverkkoihin ja käyttäjälaitteeseen, jossa mainittu käyttäjälaite pystyy olemaan samanaikaisesti yhteydessä ainakin kahteen mainituista useista runkoverkoista mainitun yhteysverkon kautta, **tunnettu** siitä, että mainittu yhteysverkko käsittää välineet erillisten salausparametrien vastaanottamiseksi mainituista runkoverkoista; ja mainittu yhteysverkko käsittää välineet yhden mainituista erillisistä salausparametreistä valitsemiseksi salaamaan liikenteen mainitun käyttäjälaitteen ja mainittujen ainakin kahden useista runkoverkoista välillä.

Patentkrav

1. Ett kommunikationsnätverk, som omfattar en användarutrustning, ett accessnätverk och ett flertal kärnnätverk, där nämnda användarutrustning har kapacitet att samtidigt kommunicera med åtminstone två av det nämnda flertalet kärnnätverk, **kännetecknat** därav, att samtliga nämnda åtminstone två av det nämnda flertalet kärnnätverk innehåller medel för kommunikation av separata chifferparametrar till det nämnda accessnätverket; och att nämnda accessnätverk innehåller medel för att välja en av de nämnda chifferparametrarna för chiffrering av kommunikationerna mellan nämnda användarutrustning och nämnda åtminstone två av det nämnda flertalet kärnnätverk.

2. Ett kommunikationsnätverk enligt patentkrav 1, **kännetecknat** därav, att nämnda accessnätverk vidare innehåller medel för chiffrering av nämnda kommunikationer mellan nämnda användarutrustning och nämnda åtminstone två av nämnda flertal kärnnätverk med den valda av de nämnda separata chifferparametrarna.

3. Ett kommunikationsnätverk enligt patentkrav 1 och 2, **kännetecknat** därav, att nämnda chifferparametrar är en chiffernyckel eller en chifferalgoritm eller en kombination av båda.

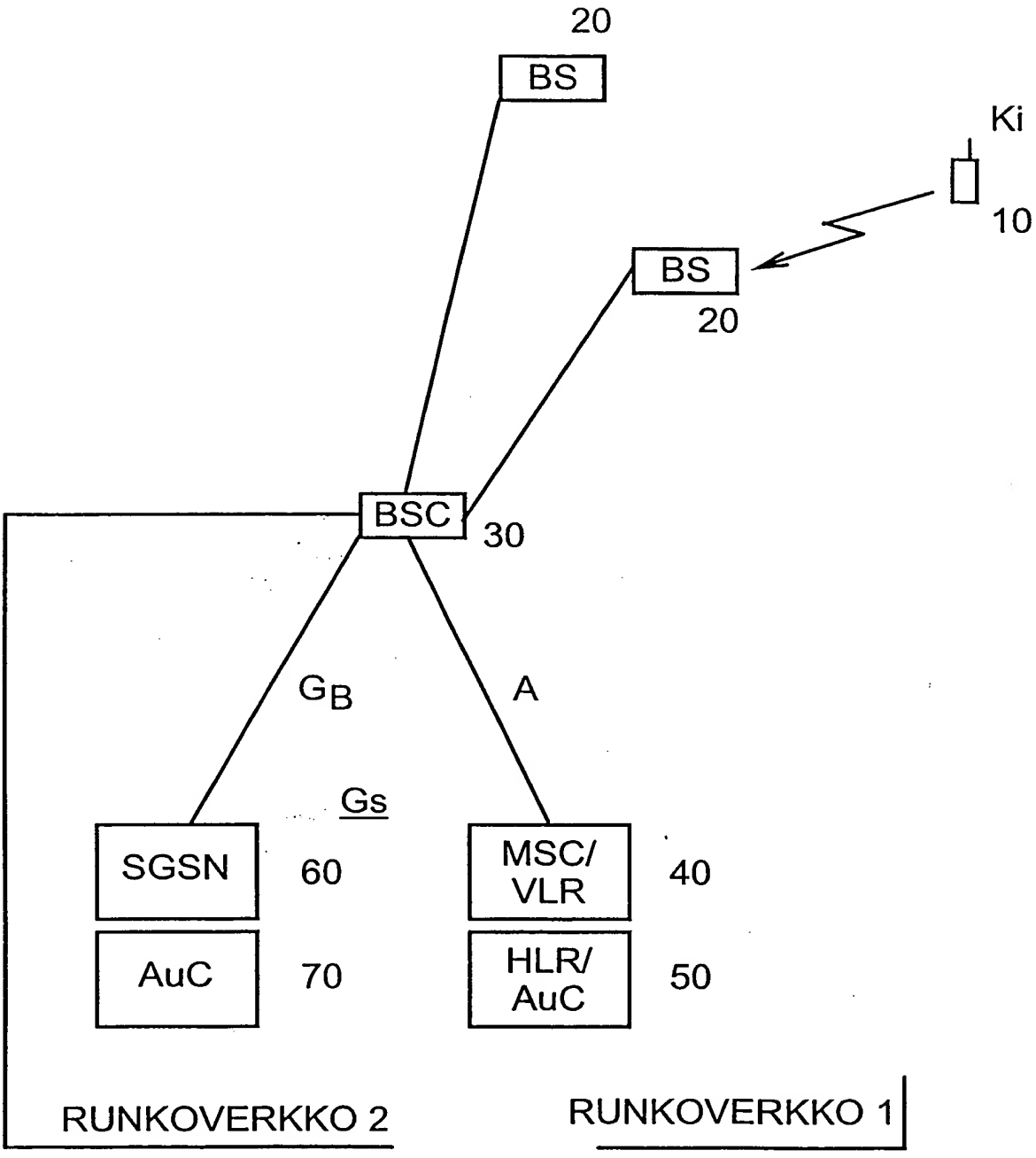
4. Ett förfarande för chiffrering i ett kommunikationsnätverk som omfattar en användarutrustning, ett accessnätverk och ett flertal kärnnätverk, där nämnda användarutrustning har kapacitet att samtidigt kommunicera med åtminstone två av de nämnda kärnnätverken, **kännetecknat** därav, att vardera av nämnda åtminstone två av de nämnda kärnnätverken kommunicerar separata chifferparametrar till nämnda accessnätverk; och att nämnda accessnätverk väljer ett av de nämnda separata chifferparametrarna för chiffrering av kommunikationen mellan nämnda användarutrustning och nämnda åtminstone två av nämnda flertal av kärnnätverk.

5. Ett förfarande för chiffrering enligt patentkrav 4, **kännetecknat** därav, att nämnda accessnätverk vidare chiffrerar nämnda kommunikation mellan nämnda användarutrustning och nämnda åtminstone två av nämnda flertal kärnnätverk med nämnda val av en av nämnda separata chifferparametrar.

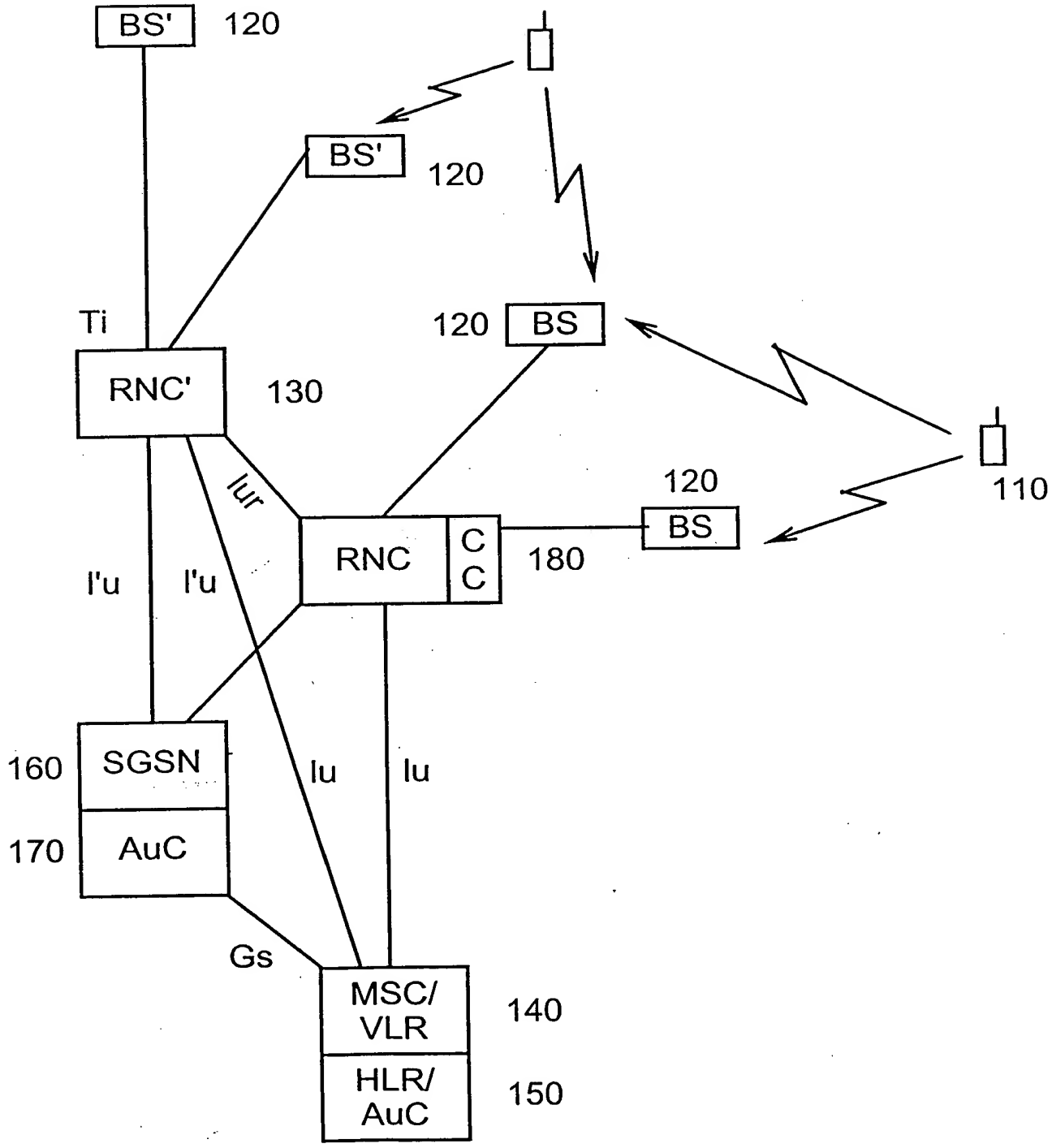
6. Ett förfarande för chiffrering enligt patentkrav 4 eller 5, **kännetecknat** därav, att nämnda chifferparametrar är en chiffernyckel eller en chifferalgoritm eller en kombination av båda.

7. Ett förfarande för chiffrering enligt patentkrav 4, **kännetecknat** därav, att nämnda accessnätverk omfattar ett flertal enheter avsedda för att hantera chiffreringen av kommunikationerna med användarutrustning placerad i ett geografisk område tilldelat nämnda respektive enhet och att när nämnda användarutrustning flyttar från ett geografiskt område tilldelat en första chifferhanterande enhet till ett geografiskt område tilldelat en andra chifferhanterande enhet så kommunicerar nämnda första chifferhanterande enhet de använda chifferparametrarna till den nämnda andra chifferhanterande enheten genom att sända signaler över nämnda åtminstone två av nämnda flertal kärnnätverk.

8. Ett accessnätverkselement i förbindelse med ett flertal kärnnätverk och med en användarutrustning där nämnda användarutrustning har kapacitet att samtidigt kommunicera med åtminstone två av nämnda flertal kärnnätverk över nämnda accessnätverk **kännetecknat** därav, att nämnda accessnätverk innehåller medel för mottagning av separata chifferparametrar från nämnda kärnnätverk; och nämnda accessnätverk innehåller medel för att välja av en av nämnda separata chifferparametrar för chiffrering av kommunikationen mellan nämnda användarutrustning och nämnda åtminstone två av nämnda flertal kärnnätverk.

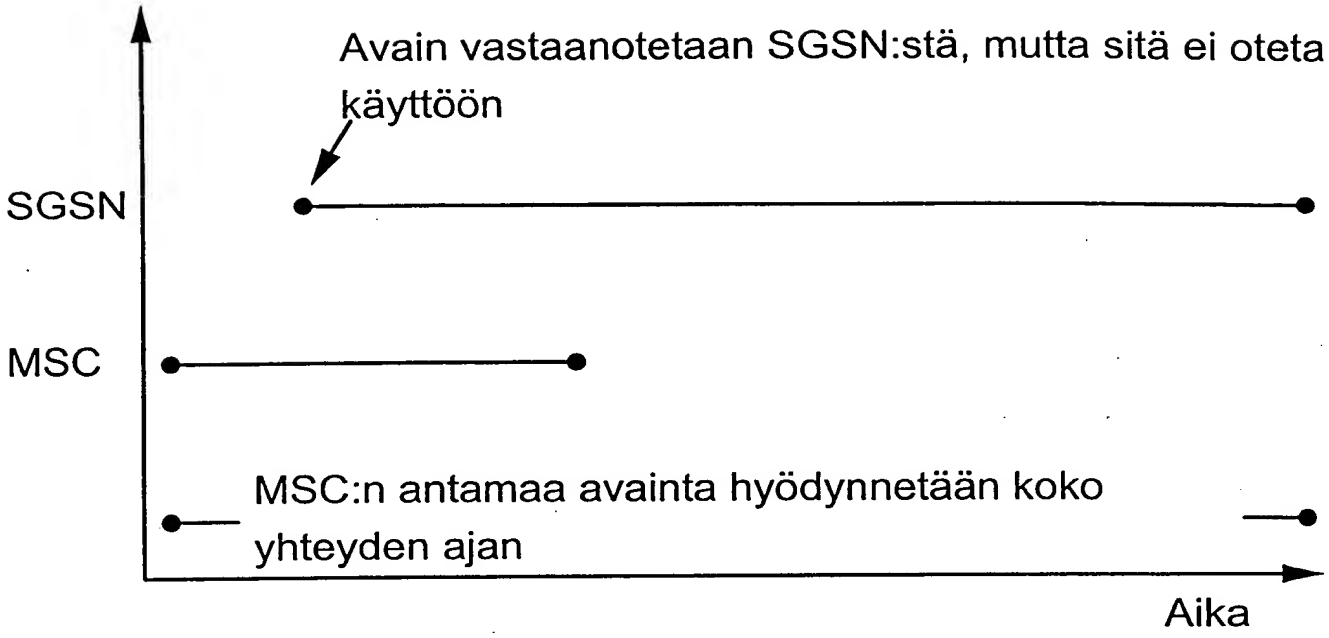

20
BS
Ki
10
BS
20
BSC
30
G_B
A
Gs
SGSN
60
MSC/
VLR
40
AuC
70
HLR/
AuC
50
RUNKOVERKKO 2
RUNKOVERKKO 1

KUVIO 1


BS'
120
BS'
120
Ti
120
BS
RNC'
130
110
120
BS
lur
RNC
C
C
180
I'u
I'u
160
SGSN
Iu
Iu
170
AuC
Gs
MSC/
VLR
140
HLR/
AuC
150

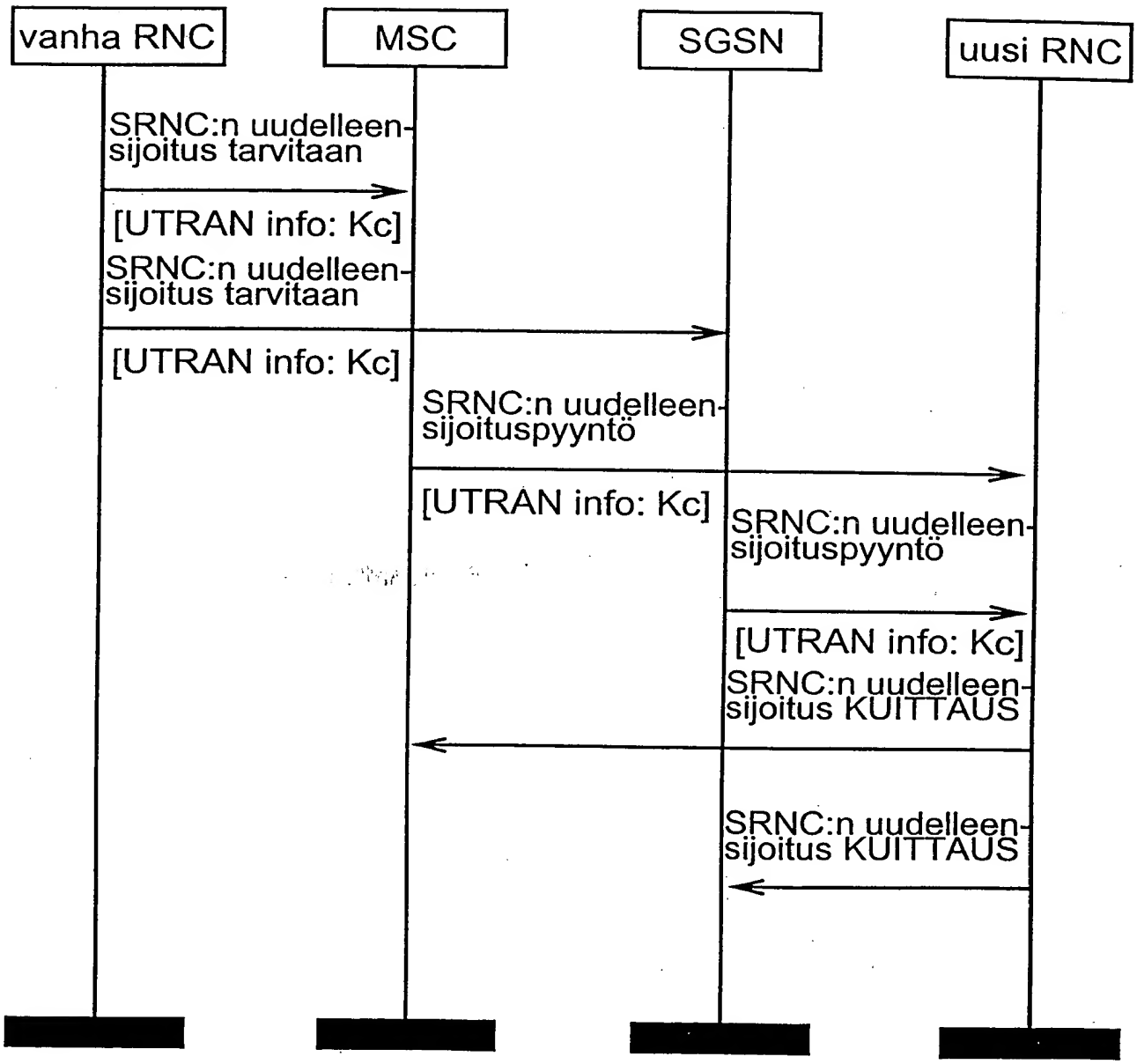
KUVIO 2

THIS PAGE BLANK (USPTO)


Avain vastaanotetaan SGSN:stä, mutta sitä ei oteta käyttöön
SGSN
MSC
MSC:n antamaa avainta hyödynnetään koko yhteyden ajan
Aika

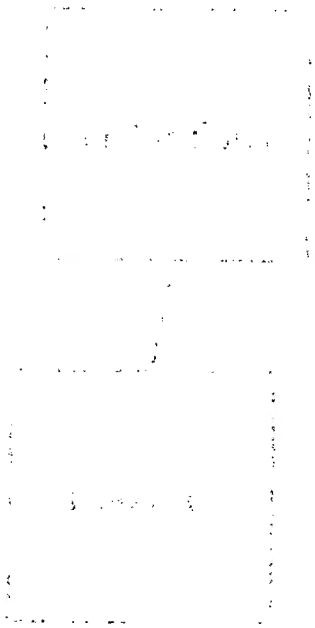
KUVIO 3

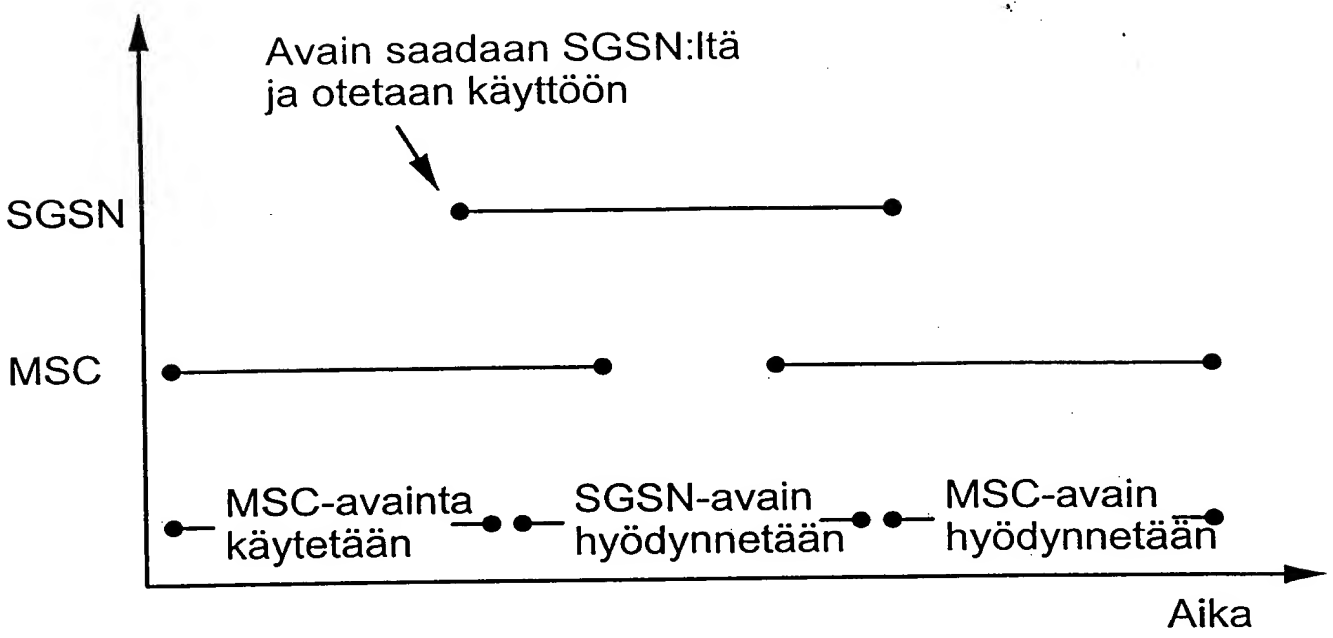
THIS PAGE BLANK (USPTO)


vanha RNC
MSC
SGSN
uusi RNC
SRNC:n uudelleen-sijoitus tarvitaan
[UTRAN info: Kc]
SRNC:n uudelleen-sijoitus tarvitaan
[UTRAN info: Kc]
SRNC:n uudelleen-sijoituspyyntö
[UTRAN info: Kc]
SRNC:n uudelleen-sijoituspyyntö
[UTRAN info: Kc]
SRNC:n uudelleen-sijoitus KUITTAUS
SRNC:n uudelleen-sijoitus KUITTAUS

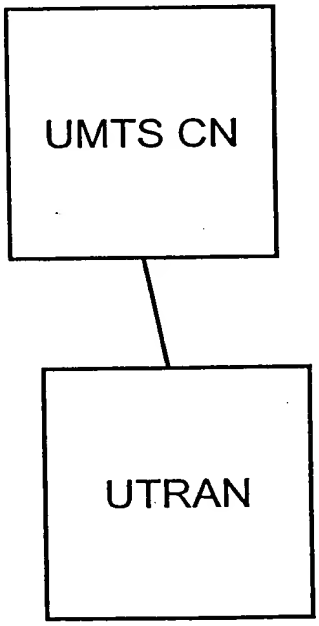
KUVIO 5

THIS PAGE BLANK (USPTO)

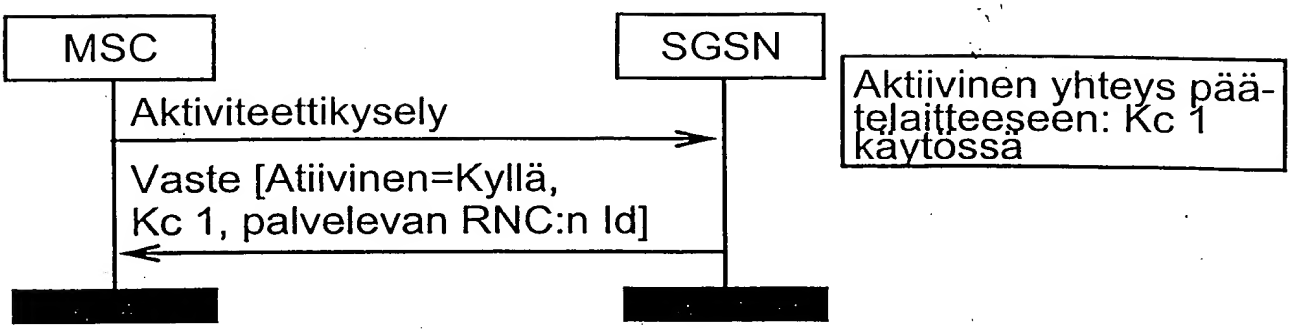




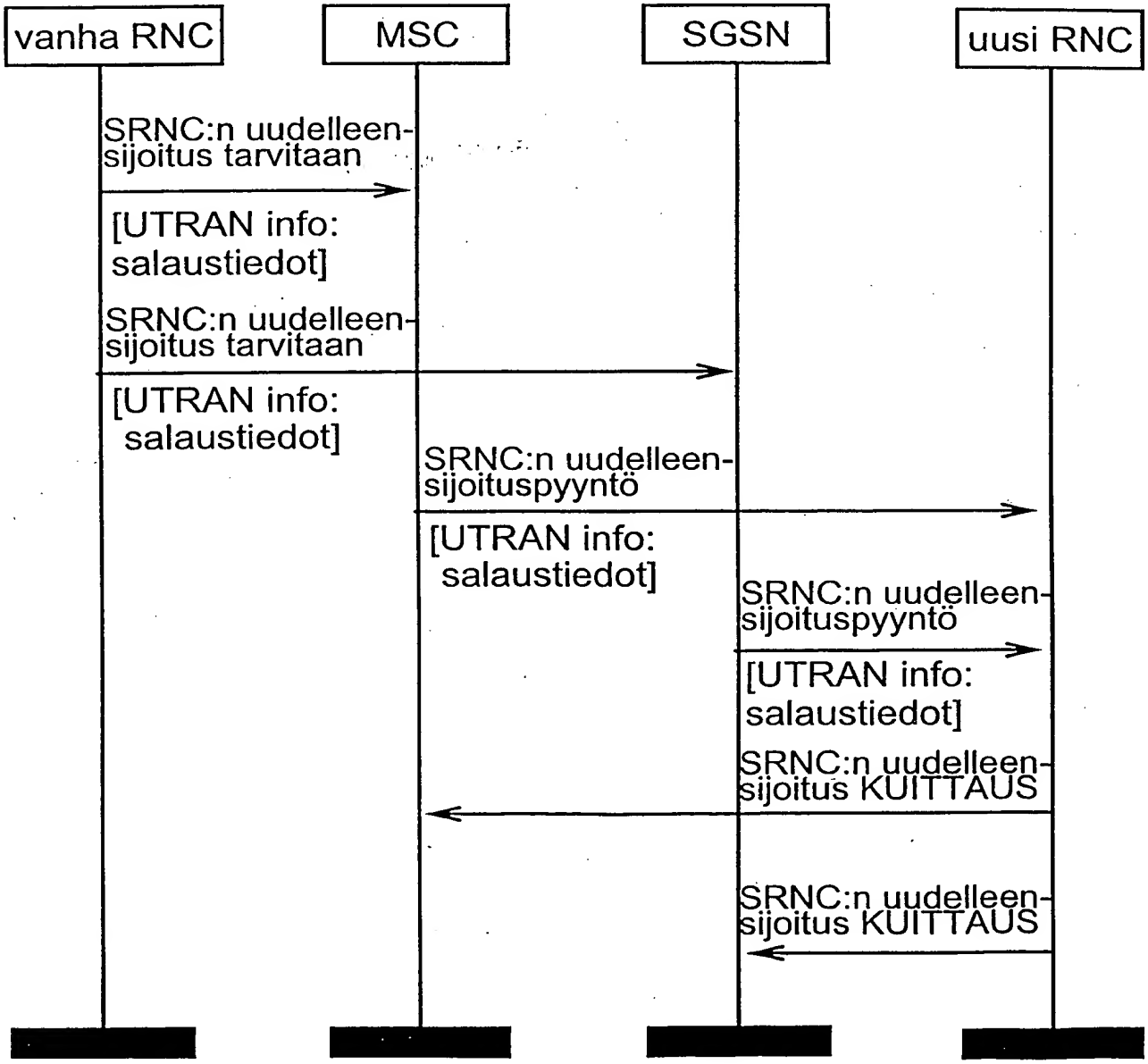
KUVIO 4



KUVIO 6



KUVIO 7



KUVIO 8